What is claimed is:

1. A method of providing a secure session key for message transmissions between first and second communication locations, said method comprising the steps of:

a) selecting a first secret number by said first communication location,

b) generating a first ephemeral number from said first secret number by said first communication location,

c) sending said first ephemeral number from said first communication location to a first proxy station,

d) selecting a second secret number by said first proxy station, and computing a first composite number from said first ephemeral number and said second secret number,

e) sending said first composite number to a second proxy station,

f) selecting a third secret number by said second proxy station, and computing a second composite secret number from said first composite number and said third secret number,

g) sending said second composite number to said second communication location,

h) selecting a fourth secret number by said second communication location, computing a second ephemeral number from said fourth secret number, and computing a third composite number from said second composite number and said fourth secret number, whereby said session key equal to said third composite number is generated at said second communication location,

i) sending said second ephemeral number by said second communication location to said second proxy station,

j) retrieving said third secret number by said second proxy station, and computing a fourth composite number from said fourth secret number and said third secret number,

k) sending said fourth composite number from said second proxy station to said first proxy station,

l) retrieving said second secret number by said first proxy station, and computing a fifth composite number from said fourth composite number and said second secret number,

m) sending said fifth composite number from said first proxy station to said first communication location,

n) retrieving said first secret number by said first communication location and recovering said session key from said fifth composite number and said first secret number at said first communication location.

2. The method of Claim 1 wherein said computing is computing modulo P in a Galois field GF(P) where P is a prime.

3. The method of Claim 2 wherein said computing modulo P comprises the steps of raising said numbers to integer exponents.

4. The method of Claim 1 wherein determining said session key at said first proxy station is not computable.

5; The method of Claim 1 wherein determining said session key at said second proxy station is not computable.

6. The method of Claim 1 including the step of exchanging challenges between said first

communication location and said second communication location.

7. The method of Claim 1 including the step of exchanging challenges comprising digitally signed certificates of authentication between said first proxy station and said second proxy station.

8. The method of Claim 1 including the step of exchanging challenges between said first communication location and said first proxy station.

9. The method of Claim 1 including the step of exchanging challenges between said second communication location and said second proxy.

10. A method of secure communication between a first and a second communication station, said method comprising the steps of:

a) said first communication station selecting a primitive element of a Galois field GF(P) where P is a prime,

b) raising said primitive element to a first exponent to compute a first number modulo P

c) transferring said first number by said first communication station to a first of at least one proxy station,

d) raising said first number to a second exponent by said first of at least one proxy station, to generate a second number modulo P,

e) transferring said second number to a second of at least one proxy station,

f) raising said second number to a third exponent by said second of at least one proxy station, to generate a third number, modulo P,

g) transferring said third number to said second communication station,

h) raising said third number to a fourth exponent by said second communication station, to generate a session key, modulo P.

11. A method of secure communication between a first and a second communication station, said method comprising the steps of:

a) said first communication station selecting a primitive element of a Galois field GF(P) where P is a prime,

b) raising said primitive element to a first exponent to compute a first number modulo P,

c) transferring said first number by said first communication station to said at least one proxy station ,

d) raising said first number to a second exponent by said at least one proxy station to generate a second number modulo P,

e) transferring said second number to said second communication station,

f) raising said second number to a third exponent by said second communication station to generate a session key, modulo P.

12. The method of Claim 10 including the step of exchanging challenges between said first communication location and said second communication location.

13. The method of Claim 10 including the step of exchanging challenges comprising digitally signed certificates of authentication between said at least one proxy station and said second communication station.

14. The method of Claim 10 including the step of exchanging challenges between said first communication location and said at least one proxy station.

15. The method of Claim 10 wherein determining said session key at said at least one proxy station is not computable.